# Indigenous.Link

Canada’s fastest growing Indigenous career portal, Careers.Indigenous.Link is pleased to introduce a new approach to job searching for Indigenous Job Seekers of Canada. Careers.Indigenous.Link brings simplicity, value, and functionality to the world of Canadian online job boards.

Through our partnership with Indigenous.Links Diversity Recruitment Program, we post jobs for Canada’s largest corporations and government departments. With our vertical job search engine technology, Indigenous Job Seekers can search thousands of Indigenous-specific jobs in just about every industry, city, province and postal code.

Careers.Indigenous.Link offers the hottest job listings from some of the nation’s top employers, and we will continue to add services and enhance functionality ensuring a more effective job search. For example, during a search, job seekers have the ability to roll over any job listing and read a brief description of the position to determine if the job is exactly what they’re searching for. This practical feature allows job seekers to only research jobs relevant to their search. By including elements like this, Careers.Indigenous.Link can help reduce the time it takes to find and apply for the best, available jobs.

The team behind Indigenous.Link is dedicated to connecting Indigenous Peoples of Canada with great jobs along with the most time and cost-effective, career-advancing resources. It is our mission to develop and maintain a website where people can go to work!

Contact us to find out more about how to become a Site Sponsor.

Corporate Headquarters:
Toll Free Phone: (866) 225-9067
Toll Free Fax: (877) 825-7564
L9 P23 R4074 HWY 596 - Box 109
Keewatin, ON  P0X 1C0

# Job Board Posting

Date Printed: 2024/06/30

Careers.Indigenous.Link

## Analyst, Operational Technology (OT) Security

| | | |
|---|---|---|
| **Job ID** | **ozZYtfwJ-14618-4294** | |
| **Web Address** | https://careers.indigenous.link/viewjob?jobname=ozZYtfwJ-14618-4294 | |
| **Company** | EPCOR | |
| **Location** | Edmonton, Alberta | |
| **Date Posted** | From: 2024-06-27 | To: 2050-01-01 |
| **Job** | Type: Full-time | Category: Utilities |

**Description**

Highlights of the jobÃ‚Â We are hiring one (1) Full-Time Permanent Analyst, Operational Technology Security position working out of Rossdale Water Treatment Plant in Edmonton, AB.Ã‚Â This opportunity isÃ‚Â open to Internal and External candidatesÃ‚Â The Operational Technology (OT) Security Analyst, working with other specialized cross-functional groups, is accountable for documenting, building, and measuring Water Services cyber security standards and programs within the boundaries of Water Services OT Cyber Security Policies and Standards.Ã‚Â In this role, you will collaborate with the Water OT Cybersecurity Manager on all tasks and responsibilities.Ã‚Â As the Analyst, you are responsible for threat and risk assessment exercises, which are completed independently and with other business unit stakeholders.Ã‚Â Other duties include following internal threat risk processes and procedures, documenting risk items in the risk register, communicating findings to stakeholders, and tracking remediation plans.Ã‚Â Including working with and guiding our Security Operations contractor to help maintain cybersecurity system monitoring tools.Ã‚Â Provide support and direction to the Security Operations contractor for any identified cybersecurity events.Ã‚Â What you'd be responsible forÃ‚Â Guiding business units to develop and maintain cybersecurity standards, procedures, and best practices documentation defined by the cybersecurity framework.Ã‚Â These duties include writing, reviewing, and managing all associated documentation.Collaborating with our partners to manage and maintain our vulnerability management program.Ã‚Â This includes reporting, advising and monitoring the business units we support.Ã‚Â Providing input to the OT cybersecurity plans and directions, and demonstrate on-going appropriate relationships with other positions, as requiredEnsuring all Water Services OT assets are properly inventoried and categorized by risk, with appropriate policies in place to ensure that systems are monitored to protect EPCOR's operational computing and communications infrastructure from malicious attacks and/or unintended changesSupporting cross functional group implementation, to create and maintain Water

Services OT device and System Cyber Security Standards for new devices (project based) and existing systems (maintenance/priority based).Multivendor systems and devices include but are not limited to; HMI's, Radio's, Data concentrators, RTU's, PLC's, DCS, Firewalls, and VPN's.Support and operation of standards covering: change management, access management, electronic security perimeter, malicious software prevention, security testing, ports and services management, patch management, security incident response, disaster recovery, audit evidence collection, and other applicable activities through ongoing and yearly update and review processes.

Perform and maintaining cyber security evaluations and for new and existing OT devices/vendors, supporting Water Service's C-SCRM programs. (Cybersecurity Supply Chain Risk Management)Working with Water Service's Security Operations contractor to manage cybersecurity investigations of any identified potential cybersecurity event.Collaborating with internal teams and support contractor to ensure the collection of OT device cyber security attributes including inventory, risk categorization, and vulnerabilities. Support with: technical and business analysis, develop business cases and participate in audits related to cyber security initiatives.Develop and maintain in-scope business units KPIs for cyber security related metrics. Participate in or drive cross-functional teams to design and maintain dashboards to support Water Services' cyber security posture.Effectively and clearly, communicate technical information both verbally and in writing to team members, management, executive, and others.Demonstrating a high performance, high discipline, safe, accountable, focused, innovative and achievement-oriented, easy to do business with manner of working.Providing input to the Operations Network and Security team plans and directions, and demonstrate on-going appropriate relationships with other positions, as required

Ã‚Â What's required to be successfulÃ‚Â 2 year post-secondary diploma in Information Technology or degree in Sciences/Computers/Engineering degree.Diploma or other relevant training/certifications in cyber security such as CISSP, CISM, CIRSC is an asset.Experience in an Operational Technology (OT) environment (SCADA) is an asset.2+ years' equivalent experience in IT/OT cyber security or related area is an asset Working experience with cyber security frameworks (C2M2, NIST CSF, CIS) is an assetExperience managing and maintaining cyber risk registers is an assetExperience leading technical cross-functional teams is an assetSecurity experience including threat identification, proactive defense, incident response, and development of mitigation strategies is an assetStrong written and verbal communication skillsRequires proficiency in business writing for the preparation of reports, standards, procedures and presentationsRequires effective presentation skills, appropriate for senior or executive management levelsExperience with business and process analysisStrong reporting and data analysis skillsetExperience managing and analyzing data from cyber security software such as baseline or vulnerability scanning toolsMaintaining training compliance as required Ã‚Â As our top candidate, you take ownership and demonstrate initiative by achieving objectives on schedule and to a defined standard. You have a keen attention to detail and are fully engaged and committed to making innovative improvements on an ongoing basis. You respond to change with an open attitude and demonstrate a willingness to learn new ways to accomplish your work and objectives. As our best candidate, you collaborate well with others and are able to deliver results, plan and organize work, and develop and meet schedules.Ã‚Â  Ã‚Â Other important facts about this jobÃ‚Â Jurisdiction: CSU52; Class: IT1Starting Wage: $48.58 (Final wage placement will be determined at the time of selection and is based on a combination of factors as outlined in the Collective Agreement that may be found online.) Hours of work: 40 hours per weekÃ‚Â Current EPCOR Employees please ensure that you are using your "@epcor.com" email address.Ã‚Â Learn more about Working at EPCOR!Follow us on LinkedIn,Ã‚Â Twitter, GlassdoorÃ‚Â or Facebook!Ã‚Â #LI-TA1Ã‚Â Please note the following information:Ã‚Â A requirement of working for EPCOR is that you are at least 18 years of age, successfully attained a high school diploma (GED, or equivalent level of secondary education) and legally entitled to work in Canada. (A copy of a valid work permit may be required.)If you are considered for the position, clearance on all applicable background checks (which may include criminal, identity, educational, and/or credit) and professional reference checks is required. Some EPCOR positions require an enhanced level of background assessment, which is dictated by law. These positions require advanced criminal record checks that must also be conducted from time to time after commencement of employment.A technical/practical assessment may be administered during the selection process and this exercise will be used as a part of the selection criterion.To meet the physical demands required of some positions, candidates must be in good physical condition and willing to work in all weather conditions. Clearance on pre-placement medical and drug and alcohol testing may be required.Prior infractions for unsafe driving behaviours will be evaluated and considered for non-selection regardless of current demerits on file.

For more information, visit EPCOR for Analyst, Operational Technology (OT) Security